form of an actual data stream, when for example a life transmission of a multimedia event is thought of. This application will especially occur with digital user-selective broadcasting.

The length of an encrypted section 16 is represented by a value amount 22 while the spacing in the encrypted multimedia data stream from the beginning of an encrypted section 16 to the beginning of the next encrypted section 16 is referred to as step 24. The length of the further encrypted section 20 is given by a value first step 26.

These values 22, 24 and 26 are obviously required for a correct decrypting of the multimedia data in a decryption device. This is why they have to be entered into the header 12 as will be explained later.

Fig.2 shows a more detailed illustration of the encrypted multimedia data stream 10 consisting of the header 12 and the payload data block 14. The header 12 is divided into several sub blocks that will be explained especially referring to Fig. 3. It is pointed out that the number and the function of the sub blocks can be extended at will. Thus, in Fig. 2 some sub blocks of the header 12 are illustrated in an only exemplary way. The header includes as it is shown in Fig. 2 a so-called crypt-block ~~29~~ 28 comprising, in general terms, relevant information for encrypting the multimedia data. In addition the header 12 includes a so-called license block 30 comprising data referring to how a user can or is allowed to use the encrypted multimedia data stream. The header 12 further includes a payload data info block 32 which can include information concerning the payload data block 14 and as well as general information about

nection with the multimedia data encryption algorithm identified by the entry 40, is required to decrypt the encrypted multimedia data (sections 16 in Fig. 1) present in the payload data block 14 correctly. In order to achieve a sufficient flexibility for future applications, the two entries output value length 48 and output value mask 50 are further provided. The entry output value length 48 illustrates the actual length of the output value 46. To achieve a flexible header format more bytes are however provided in the header format, for the output value than an output value actually comprises. The output value mask 50 thus illustrates how a shorter output value is distributed in a way on a longer output value place. If the output value length is for example half as big as the space available for the output value, the output value mask could be formed in such a way that the first half of the output value mask is set while the second half is masked. In this case the output value would simply be entered into the space provided for the header by the syntax and occupy the first half while the other half would be ignored due to the output value mask 50.

Now the license block 30 of the header 12 Fig. 2 will be explained. The license block includes an ~~entry bit mask~~ bit mask 52. This entry can comprise certain specific information for replaying or for the general way of using the encrypted multimedia data. With this entry a decryption device could especially be told whether the payload data can be replayed locally or not. In addition at this point it may be signalled whether the challenge response method has been used for the encryption, this method being described in the already mentioned German patent DE 196 25 635 C1 and enabling an efficient data base access.

than the entry allowed replay number 58. If this is the case, a decryption of the multimedia data is carried out. If this is not the case, a decryption is no longer carried out.

Analog to the entries 58 and 60 entries allowed copy numbers 62 and actual copy number 64 are implemented. By means of the two entries 62 and 64 it is made sure that a user of the multimedia data only copies them as often as he or she is allowed to do so by the provider or as often as he or she has paid for when purchasing the multimedia data. By the entries 58 to 64 a more effective copyright protection is assured, a selection between private users and industrial users being attainable for example by setting the entries allowed replay number 58 and allowed copy numbers 62 to a smaller value.

The licensing could for example be designed in such a way that a certain number of copies (entry 62) of the original are allowed while copies of a copy are not allowed. The header of a copy would then, unlike the header of the original, have zero as the entry allowed copy number in such a way that a proper encryption/decryption device can no longer copy this copy.

In the example for a multimedia data protection protocol (MMP) shown here the header 12 further contains a payload data information block 32 having in this case only two block payload data entries 66 and 68, the entry 66 containing a hash sum on the total header, while the entry 68 identifies the type of hash algorithm having been used for forming the hash sum on the total header.

For this purpose ~~author~~ other information 74 (IP information block 72) could for example count prior user information and distributor information which enables tracing back of a multimedia file which for example has been decrypted and encrypted several times by different instruments to the original provider transparently, the ~~author~~ other information 74 being maintained. It is thus possible to check at any point whether an encrypted multimedia file has been acquired legally or illegally.

Fig. 4 shows a schematic block diagram of a scenario wherein the inventive concept can be applied in an advantageous way. An author or composer 100 has created a multimedia piece, for example a text, a piece of music, a film or a picture. He delivers this work, in this invention generally referred to as multimedia piece, to a supplier 102 of multimedia data. It is especially pointed out here that the expression "multimedia data" in the sense of the present invention comprises audio data, video data or a combination of audio and video data.

The supplier ensures that the multimedia piece of the author/composer 100 is put in circulation by encoding it for example according to the method MPEG layer 3 (MP3). In order to achieve a customer selective providing for use of the encoded multimedia piece the supplier 102 will bring the encoded multimedia piece into a first data stream comprising a header and payload data block. A data stream as it might be used is illustrated in Fig. 3.

In this connection it should be especially pointed to the IP information block 72 comprising author information 74 as payload data identifying the author/composer or in general